擬素数の約数計算について (数式処理とその周辺分野の研究)

AUTHOR(S):

宮本, 泉

CITATION:

宮本, 泉. 擬素数の約数計算について (数式処理とその周辺分野の研究). 数理解析研究所講究録 2017, 2054: 139-145

ISSUE DATE:

2017-10

URL:

http://hdl.handle.net/2433/237155

数理解析研究所講究録
第2054巻 2017年 139-145

擬素数の約数計算について

宮本泉 *
IZUMI MIYAMOTO

1 はじめに

昨年度の本研究集会において、Miller-Rabin 擬素数の約数が求められる場合があることを示した。そのとき、擬素数 n に対して、$n-1$ の素因数を利用した。状況を整理すると、素因数分解法における $p-1$ 法や $p+1$ 法の適用例と考えることができると分かった。

本年度は、引き続いて、どのような素因数が利用できるかを調べた。実験対象として、本年は昨年は取扱わなかった Lucas 擬素数を取上げて、$n+1$ の素因数を利用して n の約数を求めた。$n-1$ または $n+1$ の素因数 r が利用できるのは、素数判定に使う base の order の r-part が、すべての n の素因数を法として同じにはなっていないときであることが分かった。その事実を、Lucas 擬素数のデータに対して確認をした。

2 素数判定と疑素数

自然数が素数であるかどうか判定する素数判定法は、次の 2 つの方法に大別される。

- 確定的素数判定法
- 確率的素数判定法
  「素数ではない/高い確率で素数である」を判定
  ↳素数でないとき擬素数という。

計算時間

- 確定的素数判定法→長時間かかる。
- 確率的素数判定法→短時間でできる。

【参考：(約数計算)】

- 素因数分解→困難

確率的素数判定法の例

n が奇素数で、a が $n-1$ 以下の自然数のとき次が成立する。

（すなわち、成立しなければ n は合成数である。）

*imiyamoto1@gmail.com

- $a^{n-1} = 1 \mod n$ (フェルマー法)
- $a^{(n-1)/2} = (a/n) \mod n$ (オイラーテスト), (a/n) =Jacobi(a, n) ヤコビ記号 $(= \pm 1)$
- Miller-Rabin 法 (昨年の本研究集会で取り上げた方法)

  $n - 1 = 2^s t$, t 奇数

  $a^t = \pm 1 \mod n$

  これが成立たないときは、$b = a^t$ から始めて

  $b \to b^2$ をある $k(1 \leq k \leq s-1)$ 回繰返して、$b^2 = -1$

Miller-Rabin 法による擬素数を、(a を base とする) **強擬素数**という。

2-強擬素数、2,3-強擬素数、2,3,5-強擬素数、… 小さい素数たちを base としたときの最小の擬素数が調べられている。(きりがないことが分かっている。)

3 Miller-Rabin 強疑素数の約数計算

昨年度の本研究集会ででは、強擬素数 n に対して、$n-1$ の素因数を利用して n の約数を求めた。その結果、小さい素数たちを base としたときの例で、同じ base でより大きな数まで素数判定ができるようになった。

昨年の疑問点より、

- $n-1$ の素因数の利用はいつできるのか。(⟵ これは、本年のテーマとする。)
- 合成数を base とするとき、
  - 2, 3-強擬素数なのに 6-強擬素数にはならない例があった。
  - mod n では、例えば、$4 \times 6 \mod 7 = 3$ とかなるので、base が素数であることに、意味はあるのだろうか?

  【昨年度の例より】
  - 618 桁と 1189 桁の 541 までの 100 個と 1000 までの 168 個の素数を base とする強擬素数は、それぞれ 541、1000 以下の合成数でも強擬素数となっている。(これらの例はカーマイケル数)
  - 337 桁 200 以下の素数を base とする強擬素数は、$14, 26, \cdots$ など 200 以下の合成数 22 個を base として強擬素数にはならない。

3.1 昨年紹介した方法

【例】 $n = 11718796901305940161$ (2^2 から 2^{64} までの 2-強擬素数のリストより)
$2, 3, 5, 7, 11, 13$-強擬素数、
base として 2 を使用、
$n-1$ の素因数として 13 を使用する。

- $n - 1 = 2^6 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 6737821 \cdot 12669407$
- $2^{(n-1)/32} = -1 \mod n$

- $b = 2^{(n-1)/(32\times 13)} \mod n := \mathsf{PowerMod}(2, (n-1)/32/13, n) = 272596927847311495$

$\Longrightarrow b^{13} + 1 = 0 \mod n$

$\mathsf{Gcd}(b+1, n) = 1976427493 \qquad (n = 1976427493 \times 5929282477)$

（大部分の計算実験では、baseとして、$2, 3, 5, 7$ を使用、$n-1$ の素因数としては、$3, 5, 7$ を使用していた。）

Miller-Rabin 法に従って、上の手順で計算をしていたが、実は、

$2^{n-1} = 1 \mod n$

$2^{(n-1)/13} \neq 1 \mod n$

$1 < \mathsf{Gcd}(2^{(n-1)/13} - 1, n) < n$

により、n の約数が求められる。

3.2 約数を求める方法 $p-1$ 法

昨年度の方法を、上記のように整理すると、下記の方法を適用していると考えられる。

Pratt の素数判定 (1975)

$n - 1 = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ 素因数分解が可能なとき

- $a^{n-1} = 1 \mod n$
- $a^{(n-1)/p_i} \neq 1 \mod n \quad (i = 1, 2, \cdots, r)$

$\Longrightarrow \mathbb{Z}/n\mathbb{Z}\backslash\{0\}$ が乗法に関して a を生成元とする巡回群

Pratt の素数判定の拡張（その 1）

- $a_i^{n-1} = 1 \mod n$
- $a_i^{(n-1)/p_i} \neq 1 \mod n \quad (i = 1, 2, \cdots, r)$

$\Longrightarrow \mathbb{Z}/n\mathbb{Z}\backslash\{0\}$ が乗法に関して巡回群

Pratt の素数判定の拡張（その 2）

$n - 1 = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m, \quad m < \sqrt{n}$

- $a_i^{n-1} = 1 \mod n$
- $\mathsf{Gcd}(a_i^{(n-1)/p_i} - 1, n) = 1 \quad (i = 1, 2, \cdots, r)$

$\Longrightarrow n$ は $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} (> \sqrt{n})$ 以上の素因数しかもたない

ポラードの $p-1$ 法 (1974)

第一段階

$K = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \mod n$

M は適当に大きな数として、

$p_i < M$ となる素数すべての $p_i^{e_i} < M \leq p_i^{e_i+1}$ となるべきすべての積をとる。

第二段階

$K = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} q \mod n, \quad M \leq q$ となるひとつの素数とする。

$\Longrightarrow 1 < \mathsf{Gcd}(n, a^K - 1) < n$ を期待する。

($a^K \neq 1 \mod n$ かつ $a^K = 1 \mod p$ となる n の素因数 p の存在を期待する。)

【注意】Lucas 擬素数に関しては、同様に、$p+1$ 法と呼ばれる方法がある。

3.3 $n-1$ の素因数の利用

【昨年度の引用より】

P.Beauchemin, G.Brassard, C.Crrpeau, C.Goutier, C.Pomerance(1988) などで、次のことが指摘されている。

Fermat 擬素数で強擬素数ではない場合では、Miller-Rabin 法の計算手順において

$\exists b$ such that $b \neq -1, b^2 = 1 \mod n$

となり、このとき $1 < \mathsf{Gcd}(b \pm 1, n) < n$ によって n の約数が得られる。

W. R. Alford, A. Granville, C. Pomerance(1994) Proposition 1.1.

n は a を base とする強擬素数のとき、すべての n の素因数 p に対して、

a の $\mathbb{Z}/p\mathbb{Z}$ の乗法群における order の 2-part は同じになる。

上記の引用において、Miller-Rabin 法の計算では、$n-1$ の素因数として 2 を使用していると考えられる。同様の議論によって、次の命題が得られる。

命題 n を $a^{n-1} = 1 \mod n$ となる擬素数、r を $n-1$ の素因数とする。n のある素因数 p_1, p_2 ににおいて、a の $\mathbb{Z}/p_i\mathbb{Z}, (i = 1, 2)$ の乗法群における order の r-part が等しくないならば、r の適当なべき乗 r^t に対して $1 < \mathsf{Gcd}(a^{(n-1)/r^t} - 1, n) < n$ が成立する。

4 Lucas テストと $n+1$ の素因数の利用

本年は Lucas テストを使って実験を行うことにした。Lucas テストにおいては、上の命題で $n-1$ の素因数ではなくて、$n+1$ の素因数を利用することになる。

Lucas テスト (Robert Baillie; Samuel S. Wagstaff, Jr. (1980))

$$\text{Lucas 系列 }: x_{m+2} = ax_{m+1} - bx_m \mod n$$

この数列の一般解は、2 次方程式 $x^2 = ax - b$ の 2 つの解を α, β とすると、

$$x_m = s\alpha^m + t\beta^m$$

となる。そこで、2 つの系列 $x_m = \alpha^m + \beta^m$, $y_m = (\alpha^m - \beta^m)/\sqrt{a^2 - 4b}$ を考える。初項と第 2 項は、それぞれ、$x_0 = 2$, $x_1 = a$、$y_0 = 0$, $y_1 = 1$ となる。

n が素数で、$\mathsf{Jacobi}(a^2 - 4b, n) = 1$ のとき、$\alpha, \beta \in \mathsf{GF}(n)$ なので、$\alpha^{n-1} = \beta^{n-1} = 1 \mod n$ で、

$$x_{n-1} = 2, \quad y_{n-1} = 0 \mod n$$

となって、フェルマーテストと同じになる。

n が素数で、$\mathsf{Jacobi}(a^2 - 4b, n) = -1$ のとき、$x^2 = ax - b$ による 2 次拡大体 $\mathsf{GF}(n^2)$ において、$\alpha + \beta = a$, $\alpha\beta = b$; $\alpha^n = \beta$, $\beta^n = \alpha$, $\alpha^{n+1} = \beta^{n+1} = b$ となり、特に、

$$x_{n+1} = 2b, \quad y_{n+1} = 0 \mod n$$

が成立する。したがって、これが成立しなければ、n は合成数となる。

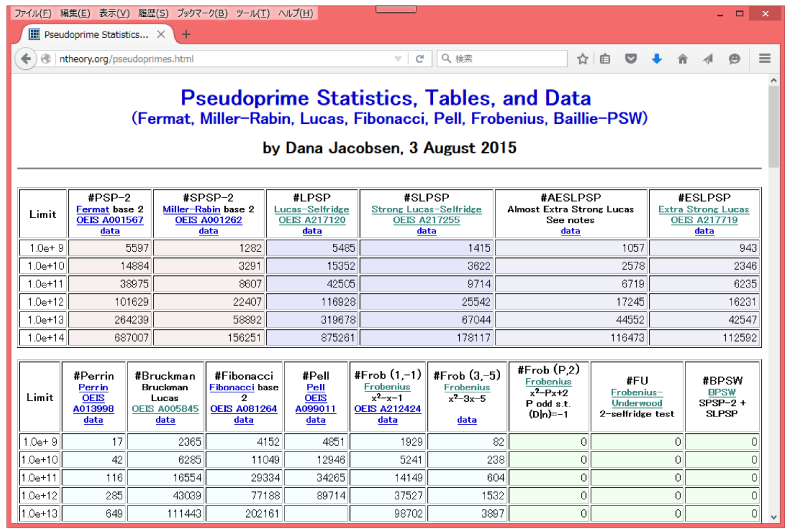
Miller-Rabin テストのときの base ごとに擬素数が定まるのと同様に、$\mathsf{Jacobi}(a^2 - 4b, n) = -1$ を満たす a,b ごとに Lucas 擬素数が定まる

GAP の Lucas 疑素数のチェックでは、$b=1$ とし、$a=2$; while Jacobi$(a^2-4,n)=1$ $a++$; により a を定めて、

$$[x_{n+1},x_n]=[2,a] \mod n$$

を計算する。この a,b の設定は、以下の Web ページに出てくる extra strong Lucas pseudo prime(ESLPSP) の設定と同じとなっている。

Miller-Rabin テストと Lucas テストたち



Pseudoprime Statistics, Tables, and Data
(Fermat, Miller–Rabin, Lucas, Fibonacci, Pell, Frobenius, Baillie–PSW)
by Dana Jacobsen, 3 August 2015

Limit	#PSP–2 Fermat base 2 OEIS A001567 data	#SPSP–2 Miller–Rabin base 2 OEIS A001262 data	#LPSP Lucas–Selfridge OEIS A217120 data	#SLPSP Strong Lucas–Selfridge OEIS A217255 data	#AESLPSP Almost Extra Strong Lucas See notes data	#ESLPSP Extra Strong Lucas OEIS A217719 data
1.0e+ 9	5597	1282	5485	1415	1057	943
1.0e+10	14884	3291	15352	3622	2578	2346
1.0e+11	38875	8607	42505	9714	6719	6235
1.0e+12	101629	22407	116928	25542	17245	16231
1.0e+13	264239	58892	319678	67044	44552	42547
1.0e+14	687007	156251	875261	178117	118473	112592

Limit	#Perrin Perrin OEIS A013998 data	#Bruckman Bruckman Lucas OEIS A005845 data	#Fibonacci Fibonacci base 2 OEIS A081264 data	#Pell Pell OEIS A099011 data	#Frob (1,–1) Frobenius x^2-x-1 OEIS A212424 data	#Frob (3,–5) Frobenius x^2-3x-5 data	#Frob (P,2) Frobenius x^2-Px+2 P odd s.t. (D|n)=–1	#FU Frobenius–Underwood 2–selfridge test	#BPSW BPSW SPSP–2 + SLPSP
1.0e+ 9	17	2365	4152	4851	1929	82	0	0	0
1.0e+10	42	6285	11049	12946	5241	238	0	0	0
1.0e+11	116	16554	29334	34265	14149	604	0	0	0
1.0e+12	285	43039	77188	89714	37527	1532	0	0	0
1.0e+13	849	111443	202161		98702	3997	0	0	0

5 計算実験

実験データは、上の Web ページより参照した。

Extra strong Lucas pseudoprime (Web ページの略記号：ESLPSP) J. Grantham (2000). "Frobenius Pseudoprimes" では、次の計算をチェックしている。

$b=1$; $a=3$; *while* Jacobi$(a^2-4,n)=1$ $a=a++$;

$n+1=2^st$, t 奇数として

$x_t=\pm 2 \mod n$ かつ $y_t=0 \mod n$

または、ある $r\leq s-1$ に対して

$x_{2^rt}=0 \mod n$

【注意】$b=1$ としたので、n が素数のとき、$\alpha^{n+1}=\beta^{n+1}=1 \mod n$ が成立し、特に、α の order($=\beta$ の order) は $n+1$ の約数になる。

【参考】almost extra strong Lucas pseudoprime では $y_t=0 \mod n$ を無視したチェックをしている。

GAP の IsBPSWLucasPseudoPrime を使って、前の Web ページで参照したのデータから、この GAP 関数で true となる数を集めて、実験データとした。その結果、

ESLPSP は true、AESLPSP\ESLPSP では false となったので、

LPSP より true な数を求めて、ESPSP と合計して 264895 個が実験データとなった。

【計算実験例 1 】$n=635627=563\times 1129$

$a=3$ で Jacobi$(3^2-4,n)=-1$ となる。

$x^2-3x+1=0$ は、 mod 563 で既約、 mod 1129 で可約。

解 α の order(= β の order) は、それぞれ、 mod 563 と mod 1129 で、
$188 = (563+1)/3 = 2\times 2\times 47$ と
$564 = (1129-1)/2 = 2\times 2\times 3\times 47$
となる。
$x_m = \alpha^m + \beta^m$ は、
$[x_m, x_{m-1}] = \mathsf{TraceModQF}(a,m,n)$ で計算できる。
order の 3-part が同じにならないので、
$\mathsf{TracwModQF}(a, n+1, n) = [2,3]$
$\mathsf{TracwModQF}(a, (n+1)/3, n) = [1128, 345685]$

gap > List([1128, 345685] − [2, 3], u–> Gcd(u, n));

[563, 563]
【計算実験例 2 】 $n = 37331945213491 = 2036663\times 18329957$
$n+1$ の約数として 5689 が必要となる。
自作の GAP プログラムにより、n の素因数 p ごとの $\mathsf{GF}(p) = \mathbb{Z}/p_i\mathbb{Z}$ または 2 次拡大体 $\mathsf{GF}(p^2)$ における α の order と体の乗法群の生成元による α および β の表記を求めた。下記がこの例における
[[n の素因数ごとの α の order], [同じく [生成元による α, β の表記]]]
となる。

```
gap> lucasPseudo(n);
[ [ 179, 1018331 ],
  [ [ ZmodpZObj( 947680, 2036663 ), ZmodpZObj( 1088979,
      2036663 ) ], [ 6490331+5919812z, 11839622+12410145z ] ] ]

gap> List(last[1],FactorsInt);
[ [ 179 ], [ 179, 5689 ] ]
gap> Jacobi(4^2-4,n);
-1
gap> TraceModQF(4,n+1,n);
[ 2, 4 ]
gap> TraceModQF(4,(n+1)/2/2,n);
[ 2, 4 ]
gap> TraceModQF(4,(n+1)/5689,n);
[ 20291259212361, 32147340524164 ]
gap> List(last-[2,4],u->Gcd(u,n));
[ 2036663, 2036663 ]
gap> TraceModQF(4,(n+1)/179,n);
[ 23917898664215, 13303253262445 ]
gap> List(last-[2,4],u->Gcd(u,n));
[ 1, 1 ]
```

以上の例は、いずれも、ESLPSP(Extra strong Lucas pseudoprime) となっている。
【計算実験例 3 】 $n = 4170664703 = 367\times 1103\times 10303$ (ESLPSP ではない例)
$m = n+1, (n+1)/2, (n+1)/4, (n+1)/8$ に対して、それぞれ、
$\mathsf{TraceModQF}(3,m,n) = [2,3],[2,3],[2,3],[2543769486, 3815654229]$
$\mathsf{List}([2543769486, 3815654229] - [2,3], u- > \mathsf{Gcd}(u,n) = [404801, 404801]$

となり、$n+1$ の素因数として 2 を利用して、n の約数を求めることができた。

計算実験の結果

Dana Jacobsen の Pseudoprime Statistics, Tables, and Data から参照したデータより、GAP の IsBPSWLucasPseudoPrime で true となる数を集めて実験対象の GAP の Lucas 疑素数とした。

	個数	説明
GAP の Lucas 疑素数	264895	
約数が得られる数	200576	
ESLPSP ではない数	152299	$n+1$ の素因数として 2 を使って約数が得られる。
約数が得られない数	64319	$\subset$ESLPSP
ESLPSP	112592	Web ページのデータ $\cup$ 下の注の数
約数が得られる ESLPSP	48277	下の注の 4 個の数を含む。

【注】ESLPSP テストでは、b を決めるまでに $n > \mathrm{Gcd}(b^2-4, n) > 1$ をチェックしている。次の数は、これによって ESLPSP のデータから除外されている。($n+1$ の素因数を使っても約数は得られる。)

$[4917219, 448908459, 15180999119, 49467979574859]$

使用した [$n+1$ の素因数, 使用回数] の一覧

```
[ [ 3, 31443 ], [ 5, 8278 ], [ 7, 4024 ], [ 11, 1306 ], [ 13, 908 ], [ 17, 477 ],
  [ 19, 421 ], [ 23, 260 ], [ 29, 163 ], [ 31, 155 ], [ 37, 104 ], [ 41, 83 ],
  [ 43, 79 ], [ 47, 73 ], [ 53, 55 ], [ 59, 26 ], [ 61, 47 ], [ 67, 23 ], [ 71, 20 ],
  [ 73, 23 ], [ 79, 13 ], [ 83, 23 ], [ 89, 16 ], [ 97, 19 ], [ 101, 12 ],
  [ 103, 12 ], [ 107, 13 ], [ 109, 13 ], [ 113, 7 ], [ 127, 8 ], [ 131, 7 ],
  [ 137, 6 ], [ 139, 9 ], [ 149, 7 ], [ 151, 4 ], [ 157, 10 ], [ 163, 3 ], [ 167, 4 ],
  [ 173, 5 ], [ 179, 9 ], [ 181, 6 ], [ 191, 4 ], [ 193, 4 ], [ 197, 2 ], [ 199, 4 ],
  [ 211, 3 ], [ 223, 2 ], [ 227, 1 ], [ 229, 3 ], [ 233, 1 ], [ 239, 3 ], [ 241, 4 ],
  [ 251, 2 ], [ 263, 1 ], [ 269, 1 ], [ 271, 3 ], [ 281, 3 ], [ 283, 2 ], [ 293, 2 ],
  [ 307, 1 ], [ 313, 3 ], [ 317, 2 ], [ 331, 2 ], [ 337, 1 ], [ 353, 2 ], [ 359, 2 ],
  [ 421, 3 ], [ 439, 2 ], [ 461, 2 ], [ 463, 1 ], [ 499, 2 ], [ 509, 2 ], [ 521, 2 ],
  [ 547, 1 ], [ 557, 1 ], [ 563, 1 ], [ 569, 1 ], [ 571, 1 ], [ 587, 1 ], [ 593, 1 ],
  [ 613, 1 ], [ 617, 1 ], [ 619, 1 ], [ 631, 1 ], [ 647, 1 ], [ 659, 2 ], [ 727, 1 ],
  [ 757, 1 ], [ 809, 1 ], [ 859, 1 ], [ 919, 1 ], [ 991, 1 ], [ 1303, 1 ],
  [ 1327, 1 ], [ 1433, 1 ], [ 1627, 1 ], [ 1721, 1 ], [ 1861, 1 ], [ 2357, 1 ],
  [ 2389, 1 ], [ 2411, 1 ], [ 2647, 1 ], [ 5689, 1 ] ]
```

6 まとめ

擬素数 n に対して、$n-1$ や $n+1$ の素因数を使って n の約数を求めることができるのはどのようなときであるのかが分かった。この事実を、Lucas 擬素数のデータに適用して確認した。

Lucas 擬素数のうちで、extrastrongLucas 擬素数 (ESLPSP) となるのは半分よりかなり少ない、すなわち、$n+1$ の素因数として 2 を利用して n の約数を求めることに相当することで、擬素数のうち半分よりかなり多くが素数でないと判定できることになる。しかし、そのあとで、利用可能な $n+1$ の素因数すべてを利用しても、約数が得られて n が素数ではないと判定できるのは、ESLPSP のうちの半分以下になっていて、効率が悪い。また、$n+1$ のいくつかの素因数を同時に利用する良いアルゴリズムも見つかっていない。